

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-006784

(43)Date of publication of application : 12.01.1996

(51)Int.Cl.

G06F 9/06
G06F 13/00
G09C 1/00

(21)Application number : 06-132675

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 15.06.1994

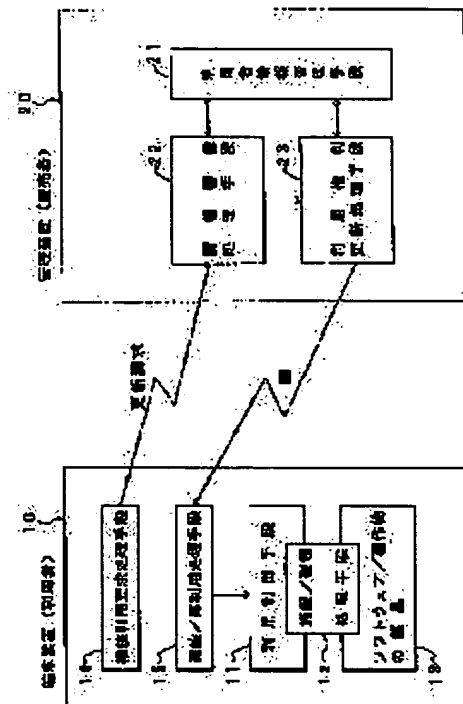
(72)Inventor : OTSUJI SEITA
KASAHARA HISATSUGU

(54) SYSTEM AND PROCESSING METHOD FOR PREVENTING USING OF UNAUTHORIZED COPY OF SOFTWARE/WORK

(57)Abstract:

PURPOSE: To prevent convenience for the sales of software and work via a line from being impaired, to prevent the unauthorized copy of them from being performed without requiring a complicated procedure and to easily cope with trial for a certain period.

CONSTITUTION: A marketable product 13 of software/work on which a lock/ destruction processing means 12 is provided and a key are sent to the purchased terminal equipment 10 of a user via a communication channel. Purchased software, etc., can be used by unlocking in the terminal equipment 10. When an expiration date arrives, the software or work is automatically locked or destroyed, then, an operation can be stopped. The user receives a new key or marketable product 6 requesting update to a managing device 20 by a continuous use request processing means 14, and continues the use of the purchased software or work until the next expiration date by unlocking the key by an unlocking/reuse processing means 15. Such operation is continued as far as the software or work is used continuously.



LEGAL STATUS

[Date of request for examination] 08.03.2000

[Date of sending the examiner's decision of rejection] 15.07.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-6784

(43)公開日 平成8年(1996)1月12日

(51)Int.Cl. ⁹	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0 C	7230-5B		
	L	7230-5B		
13/00	3 5 1 Z	7368-5E		
G 0 9 C 1/00		7259-5J		

審査請求 未請求 請求項の数2 O L (全 8 頁)

(21)出願番号 特願平6-132675

(22)出願日 平成6年(1994)6月15日

(71)出願人 000004226

日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(72)発明者 大辻 清太

東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内

(72)発明者 笠原 久嗣

東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内

(74)代理人 弁理士 小笠原 吉義 (外1名)

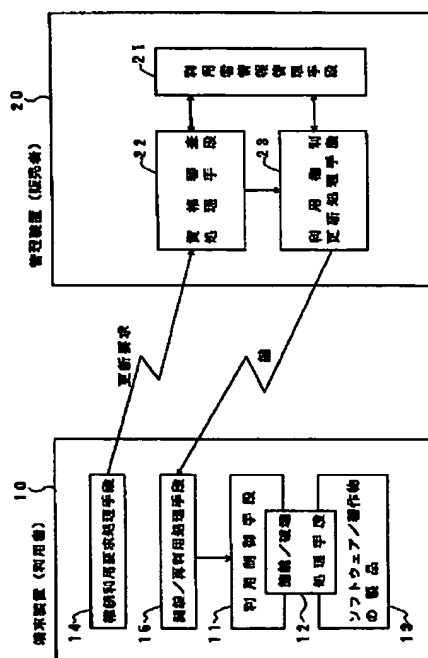
(54)【発明の名称】 ソフトウェア／著作物の無断複製使用防止システムおよび無断複製使用防止処理方法

(57)【要約】

【目的】回線経由でソフトウェアや著作物を販売する利便性を損なわず、煩雑な手続きを必要としないで、不正複製を防止することを可能にし、またある期間の試用などに容易に対処できるようにすることを目的とする。

【構成】購入した利用者の端末装置10に、施錠／破壊処理手段12を施したソフトウェア／著作物の製品13と鍵とを通信回線経由で送る。端末装置10では、その鍵を用いて購入したソフトウェア等を開錠して使用する。有効期限がくればソフトウェアまたは著作物は自動的に施錠または破壊されて作動を停止する。利用者は、継続利用要求処理手段14により管理装置20に対し更新を要求することにより、新しい鍵または製品を受け、開錠／再利用処理手段15により開錠して次の有効期限まで購入したソフトウェアまたは著作物の利用を継続する。以上を継続利用する限り繰り返す。

実施例のシステム構成図



【特許請求の範囲】

【請求項1】 ソフトウェアまたは著作物の製品を利用するための利用制御手段を有する1または複数の端末装置と、前記ソフトウェアまたは著作物の製品を利用する利用者情報を管理し、前記端末装置に通信回線を介して接続可能な管理装置とからなり、前記ソフトウェアまたは著作物の製品またはその製品の利用制御手段には有効期限の経過により自動的に前記ソフトウェアまたは著作物の製品を利用不能とする施錠／破壊処理手段が組み込まれ、前記端末装置は、前記管理装置に対して前記ソフトウェアまたは著作物の製品を利用する権利の更新を要求する継続利用要求処理手段と、前記管理装置から継続利用が認められて送られた鍵またはその製品本体の一部もしくは全部により、前記ソフトウェアまたは著作物の製品を利用可能とする開錠／再利用処理手段とを備え、前記管理装置は、前記端末装置からの継続利用要求に対し利用者情報によって利用資格を審査する資格審査処理手段と、審査に合格し利用権利を更新する場合に前記ソフトウェアまたは著作物の製品を利用可能とするための鍵またはその製品本体の一部もしくは全部を前記端末装置へ通信回線経由で送信する利用権利更新処理手段とを備えたことを特徴とするソフトウェア／著作物の無断複製使用防止システム。

【請求項2】 通信回線を用いて販売されるソフトウェアまたは著作物の製品に関する無断複製使用防止処理方法であって、購入した利用者の端末装置に、ソフトウェアまたは著作物の製品本体と利用者個人を判定する情報・有効期限・利用条件を持つ鍵とを通信回線経由で送る第1の過程と、利用者の端末装置ではその鍵を用いて購入したソフトウェアまたは著作物を開錠して使用し、有効期限がくればソフトウェアまたは著作物は自動的に施錠または破壊されて作動を停止し、利用者が継続利用を希望する場合には有効期限の経過前または経過後に販売者の管理装置に対し更新手続を行う第2の過程と、販売者の管理装置ではそれを受けて新しい鍵または前記ソフトウェアもしくは著作物の製品本体の一部もしくは全部を利用者の端末装置に通信回線経由で送る第3の過程と、利用者の端末装置では次の有効期限まで購入したソフトウェアまたは著作物の利用を継続する第4の過程とを有し、前記第2の過程から前記第4の過程までを継続利用する限り繰り返すことを特徴とするソフトウェア／著作物の無断複製使用防止処理方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、コンピュータプログラムや、映画その他の伝統的な著作物の複製を防止するためのシステムまたは方法であって、特に通信回線を用いてセンターの管理装置と定期的に接続し、利用権利の更新をしなければ購入した製品が利用不能になるようにしたソフトウェア／著作物の無断複製使用防止システム

および無断複製使用防止処理方法に関する。

【0002】

【従来の技術】コンピュータプログラムであるソフトウェア、さらにビデオや音楽など伝統的な著作物の無断複製防止のために、従来様々な手法が提案されている。

【0003】例えばソフトウェアの保護では、次のような方法が考えられている。

① ハードウェアプロテクトによる方法（特殊なハード等の有無、インストールするハードディスク（HD）限定、ハードウェアのシリアル番号の検査）。

【0004】② フロッピーディスク（FD）プロテクトによる方法（オリジナルFDの有無。オリジナルFDは通常の複製操作では複製できない規格外方法で、鍵となる情報が記述されている）。

【0005】③ マニュアルプロテクトによる方法（起動時に質問があり、ソフトウェアに付属するマニュアルやプロテクト用の冊子に記載された情報を用いて開錠する。質問は毎回変更される）。

【0006】④ ネットワークプロテクトによる方法（LANに接続されるコンピュータのソフトウェア等で用いられ、ネットワーク上に許可された個数以上の同一シリアルナンバーを持つソフトウェアが稼動していれば動作しない）。

【0007】⑤ オーサライズによる方法（インストールできる回数を制限し、専用のツールでオリジナルのFDからソフトウェアをインストールしたHDへ、複製利用権を表わすファイルを転送する。起動時に複製利用権の有無を検査）。

【0008】その他、良心に訴える方法として記名制（毎回起動時に許諾された者の名前などが表示される）、シリアルナンバー記入制（最初の起動時に、ソフトウェアのシリアルナンバー入力を要求し、入力しないと起動しない。入力によりソフトウェアにシリアルナンバーが格納されるので、不正複製された場合、誰に販売したものかを追跡できる。この手法ではソフト生産時に一意なシリアル番号を個別に付与する必要がない）等がある。

【0009】また、ビデオや音楽では、アナログではレンタルビデオにコピーガード等の品質劣化処理を加える事でダビング時に画質が大きく劣化するような方法が実用化されている。さらに、複製が深刻な問題となるデジタルでは、最初から規格としてコピー防止のシステムを組み込む方法が実用化、普及している。DAT、CD等ではSCMS（シリアルコピーマネジメントシステム）が採用され、音楽情報に付属するコピー管理情報を使って孫コピーを防止している。

【0010】

【発明が解決しようとする課題】将来、回線経由でソフトウェアや著作物が販売されることが多くなると考えられる。この場合にも無断複製を防止する機構は重要であ

る。

【0011】その方法として、各ソフトウェアに応じて端末に鍵となる特殊なハードウェアを取り付けるのは、各ソフトウェア会社からハードウェアの郵送が必要であり、回線経由の販売の利便性を損なう。また、FDプロテクトは、毎回オリジナルのFDが必要となるため不便であるとともに危険であり、FDは郵送しなくてはならない。マニュアルプロテクトも使用の度に開錠する手間がかかり、かつ文書を郵送しなくてはならない。ネットワークプロテクトは、ソフトウェア起動の度に回線上での検査を要し、かつ回線から切り離して使用する場合は機能しない。オーサライズは複製回数を管理するマスターのFDが別に必要である。

【0012】このため、従来の手法では、回線経由でソフトウェアを販売する利便性を損なわないまま、不正複製を防止することは困難である。また使用装置の同一性を確認するのは一般に難しく、煩雑な手続きを必要とする。

【0013】また、少しだけ使ってみたい、ある期間だけでいいから安く使ってみたいなど、様々なレベルの利用要求に適切なコストで対処することができない。また、SCMS（シリアルコピーマネージメントシステム）は、使用機器にあらかじめ特殊なハードウェアを組み込む必要があり、汎用のコンピュータにすべて取り付けるのは事実上困難である。またコンピュータは各自に必要な装置を組み込んで使用するという性格上、SCMSを外す装置の組み込みが容易であると考えられる。またソフトウェアの手段でもSCMSのコードを変更することができるとい問題がある。

【0014】本発明は上記問題点の解決を図り、回線経由でソフトウェア等を販売する利便性を損なわず、煩雑な手続き必要としないで、不正複製を防止することを可能にし、またある期間の試用などに容易に対処可能にすることを目的とする。

【0015】

【課題を解決するための手段】ソフトウェアや著作物の販売者をA、購入者をBとする。なお、説明を分かりやすくするために、A、Bで説明するが、実際に動作するのはそれぞれ販売者の計算機と利用者の計算機等の装置である。

【0016】Aはソフトウェア／著作物を回線経由で販売する。利用者Bが購入を希望するとき、BはAに対し、回線経由で利用申し込みを提出する。この利用申し込みには、BがBであると判定できる個人情報（住所、名前、装置の情報など）を含んでいる。

【0017】Aはこれを審査し、合格すれば、Bの個人情報を用いて要求された使用条件と期間に相当する鍵を一意に作成する。Aは料金と引き換えにソフトウェアまたは著作物の製品本体と鍵とを回線経由でBに送る。

【0018】Bは期限付の鍵を用いることで、購入した

ソフトウェア等を使用できる。有効期限が来ると、Bの購入物は自動施錠や破壊により使用不能になる。ここでさらに使いたければ、Aに対し継続利用申請を回線経由で行う。この申請によりAは次の期限まで有効な鍵を同様な方法で作成し、Bに渡す。この時Aは必要に応じて、Bに対しバグ修正やメンテナンス、改良、利用条件の変更、バージョンアップサービスを行う。

【0019】このようにソフトウェア等の使用を期限にし、必要があれば定期的に更新する手段を設ける。

10 【0020】

【作用】したがって、回線上で販売したソフト等を複製しても、期限が来れば使用不能となり複製使用ができない。また、その更新手続きは登録者以外では不可能である。よって、鍵に相当するものを郵送することなく、つまり回線での販売の利便を損なうことなく、正規の購入者には最良のメンテナンスサービスを提供しながら、かつ不正利用者の複製利用を時限的に防止することが可能となる。この際の複製利用は、ネットワークプロテクトと異なり、回線から独立していても有効である。

20 【0021】

【実施例】図1は本発明の実施例のシステム構成図である。ソフトウェアまたは著作物を利用する利用者の端末装置10は、ソフトウェアまたは著作物を販売する管理装置20に、通信回線を介して接続可能になっている。

30 【0022】端末装置10は、購入したソフトウェア／著作物の製品13を利用するための利用制御手段11を有する。この利用制御手段11は、例えば購入した製品がソフトウェアプログラムの場合にはそのプログラムの起動制御手段、映像の著作物であれば表示制御手段、また音楽等の著作物であれば音声出力制御手段等である。これらは、あらかじめ端末装置10に設けられていてもよく、また購入した製品に付属した形でその都度提供されるようになっていてもよい。

40 【0023】端末装置10の利用制御手段11またはソフトウェア／著作物の製品13には、購入した製品の有効期限が経過すると自動的に施錠または一部の破壊によりソフトウェア／著作物の製品13を利用不能とする施錠／破壊処理手段12が組み込まれている。また、端末装置10は、管理装置20に対してソフトウェア／著作物の製品13を利用する権利の更新を要求する継続利用要求処理手段14と、管理装置20から継続利用が認められて送られた鍵またはその製品本体の一部もしくは全部により、ソフトウェア／著作物の製品13を利用可能とする開錠／再利用処理手段15とを持つ。

【0024】管理装置20は、利用者情報管理手段21により、ソフトウェア／著作物の製品13を購入した利用者個人を判定する情報、有効期限、その他の利用条件等を管理する。管理装置20は、端末装置10の継続利用要求処理手段14からの継続利用要求（更新要求）に対し、利用者情報管理手段21の利用者情報を参照して

正規な購入者であるかなどの利用資格を審査する資格審査処理手段22と、その審査に合格した場合に施錠または破壊したソフトウェア／著作物の製品13を利用可能とするための鍵またはその製品本体の一部もしくは全部を端末装置10へ通信回線経由で送信する利用権利更新処理手段22とを持つ。

【0025】動作は以下のとおりである。管理装置20は、ソフトウェア／著作物の製品13を購入した利用者の端末装置10に、その製品本体と利用者個人を判定する情報・有効期限・利用条件を持つ鍵とを通信回線経由で送る。また、利用者情報管理手段21にそれらの情報を登録しておく。

【0026】利用者の端末装置10では、送られた鍵を用いてソフトウェア／著作物の製品13を開錠し、有効期限がくるまで利用制御手段11によってソフトウェア／著作物の製品13を利用する。有効期限がくればソフトウェア／著作物の製品13は自動的に施錠または一部もしくは全部の破壊により作動を停止するようになっている。利用者が継続利用を希望する場合には、有効期限の経過前または経過後に販売者の管理装置20に対し、継続利用要求処理手段14により更新手続を行う。

【0027】販売者の管理装置20では、それを受けて資格審査処理手段22により利用資格を審査し、審査に合格すれば利用権利更新処理手段23によって新しい鍵またはソフトウェア／著作物の製品13本体の一部もしくは全部を利用者の端末装置10に通信回線経由で送る。また、利用者情報管理手段21の利用者情報を更新する。

【0028】利用者の端末装置10では、開錠／再利用処理手段15によりソフトウェア／著作物の製品13を再度利用可能にし、次の有効期限までソフトウェア／著作物の製品13の利用を継続する。これらの処理を継続利用する限り繰り返す。

【0029】これによって端末装置10は、通信回線を用いて管理装置20と定期的に接続し利用権利の更新をしなければ、ソフトウェア／著作物の製品13が利用不能になり、不正試用が防止されることになる。

【0030】次に、本発明のさらに具体的な実施例について図2を参照して説明する。以下の例では、コンピュータのソフトウェアを販売する場合を説明するが、これは映画や写真、文章など伝統的な著作物、また住所録や調査資料など事実に基づく著作物でもよい。

【0031】ソフトウェアの販売者をA、利用者（購入者）をBとする。

（1）ソフトウェアの利用契約

販売者Aはソフトウェアを回線経由で販売する。パソコン通信の掲示板などで、販売したいソフトウェアの宣伝を行う（処理30）。利用者Bが必要に応じて資料請求を行うと（処理31）、販売者Aは請求を受け付けて（処理32）、要求された資料および申込書を通信回線

を介して送付する。

【0032】利用者Bが購入を希望するとき、利用者Bは販売者Aに対し、回線経由で利用申し込みを提出する（処理33）。この利用申し込みは、利用者Bが後に正当な購入者（利用者B）であると判定できる個人情報（住所、名前、装置の情報など）を含んでいる。

【0033】個人情報の要求は、ソフトウェアの価格や機能から要求された鍵の性能に応じて、その詳しさが変わってよい。例えば宣伝としての性格の強い試供品では個人情報要求をなくし、有効期限だけの鍵を用いる。

【0034】販売者Aはこれを審査し（処理34）、合格すれば、利用者Bの個人情報を用いて要求された使用条件と期間に相当する鍵を一意に作成する（処理35）。

（2）鍵の作成

鍵は以下の判定が可能になるような情報を含み、かつ暗号化した形で用意する。なお、暗号化による各種セキュリティに関する技術自体は周知であるので、その暗号化等についての詳しい説明は省略する。

【0035】(a) 有効期限の判定

ソフトウェアの有効期限を判定するには時計が必要である。もし回線に接続され、回線上に基準となる時計があればそれを優先して用いる。回線から切り離されている場合には、装置の持つ時計を用いる。装置固有の時計は、端末利用者によって意図的に有効期限内に戻すなどの処理がなされることも考えられるので、最初にインストールされた日時からその後起動される毎に時計を検査し、後戻りがあると失格とする。また起動回数も同時に検査し、常識的な使用から考えられる上限を越えると失格とする。

【0036】ソフトウェアは起動されたとき、まず鍵を探して読み込む。その後、鍵から利用条件を解読し、その条件を検査する。そして検査に合格すれば起動し、失格すればその旨利用者に表示して終了する。なお有効期限については、更新時期が近づいた段階で立上時に案内するとよい。

【0037】なお検査は起動後も定期的、あるいはイベント駆動（書類の印刷など特定の機能を使用するときに検査する）で行うとより安全である。有効期限は料金、ソフトウェアの機能等に応じて設定すればよい。例えば試供品のような場合には機能を限定し、一週間程度の有効期限で無料または低価格にすれば、広く試用してもらうことができる。一方長期使用ユーザーで、その人に渡しているソフトウェアが過去に複製されたことがないなどの実績がある場合には、有効期限を1年にする、等が考えられる。

【0038】(b) 使用装置の判定

契約した利用条件が装置を限定する場合、使用装置の同一性判定が必要である。ソフトウェアから装置固有の情報を取り出せれば、起動時の判定に用いる。例えばイー

サードネットを用いている場合には、イーサネットアダプターにmac番号が一意に決まっており、これはソフトウェアで読むことができるので、これを判定に用いる。その他、たとえ一意に決めることができなくても、ある程度装置を限定できる情報（装置の形式やハードディスクのラベル名など）がソフトウェアから読み出すことができればそれを判定条件に用いる。ただし、後に装置構成の変更などにより変化する情報については、用いるのを避けるか、変更の度に鍵を再発行する。

【0039】ソフトウェアから装置固有の情報が十分に読み出せない場合には、信頼性は劣るが、使用者の個人情報をもとに作成した不可視属性のファイルを装置のIDとして、鍵との判定条件として用いる。この方法を用いる場合、複数台に使用許可を与えることもできる。所定のインストール作業によりこの不可視属性ファイルを許可したい装置に格納する。

【0040】(c) 解読防止

解読を完全に防止するのは不可能であるが、実用上は、解読がコストに見合わなければよい。つまり解読がある程度困難で、汎用性がなく、寿命が限られていれば実用上問題はない。安価なソフトウェアには簡単な鍵を、高額なソフトウェアには複雑かつ特殊な鍵を用いる。また鍵の機構は各ソフトウェア会社、さらには各ソフトウェア毎に独自に設計すれば、解読による被害の広がりを最小限にできる。また必要があればソフトウェアの利用更新手続の際に改良、変更を加えることができるので、状況の変化に柔軟に対応できる。

【0041】(3) ソフトウェアの機能制限

機能制限とは、利用者にとって必要かつ最適なものだけを提供することである。これにより、利用者Bは不必要なコストを払わずに済み、かつ自分の装置環境、用途に合ったソフトウェアを構築できる利点がある。また販売者Aは、利用者の要求情報を入手でき、かつ各個人別にソフトウェアが異なるので、不正複製を減少させることができる。

【0042】利用条件において、ソフトウェアの機能制限に関するものは、鍵で管理しても、本体を機能限定して作成してもよい。前者の方が後に利用条件を変更しても鍵の変更だけで柔軟に対処できるが、鍵の偽造により利用者が不正に利用条件を変更する危険性がある。

【0043】(4) ソフトウェアの転送

販売者Aは料金と引き換えに利用者登録を行い（処理36）、ソフトウェア本体と鍵を回線経由で利用者Bに送るか、または遠隔インストールを行う。

【0044】利用者Bは期限付の鍵を用いることでソフトウェアを開錠し（処理37）、購入したソフトウェアを起動、使用できる（処理38）。また、利用者Bは正規の登録者であるから、問題が発生したとき、所定のセンターに接続すれば随時メンテナンス等のアフターケアサービスを受けることができる（処理39）。

【0045】(5) 利用許諾の更新

有効期限が来ると、ソフトウェア自動施錠（処理40）等により利用者Bの購入物は使用不能になる。

【0046】使用不能については次のような方法が考えられる。

1. ソフトウェア本体はそのまま保存され、単に起動しない。

2. ソフトウェア自体が自己破壊・消滅する。

【0047】3. ソフトウェアが自己暗号化する。

10 また、条件によって状態が推移してもよい。例えば銀行のキャッシュカードのように、使用できない鍵で起動しようとしたとき、3回までは何も起こらないが、それ以上起動しようすると自己破壊または暗号化する方法もある。

【0048】ここでさらに使いたければ、販売者Aに対し更新申し込みにより継続申請を回線経由で行う（処理41）。利用者Bから申請を受けた販売者Aは、審査の上（処理42）、次の期限まで有効な鍵を同様な方法で作成し（処理43）、利用者Bに渡す。

20 【0049】更新の際にソフトウェア本体も何らかの情報を新たに書き加え、それに対応した情報を鍵に含めれば、本体を不正複製した者が何らかの方法で新しい鍵を入手しても、開錠できないので安全性が高まる。

【0050】もし利用者Bのソフトウェアが破壊・消滅していれば、本体も転送する。自己暗号化している場合には復号するソフトウェアを送るか、回線経由で遠隔操作して復号する。

【0051】販売者Aは更新時に必要に応じて、利用者Bに対しバグ修正やメンテナンス、改良、利用条件の変更、バージョンアップサービスを行う（処理44）。利用者Bの端末装置10では、送られた鍵によりソフトウェアを開錠し（処理45）、利用可能にする。以後、次の有効期限がくるまで、ソフトウェアを利用し、またメンテナンス等のサービスを受けることが可能になる。

【0052】以下期限が来る度に、以上の処理を繰り返す。

(6) 不正使用

利用者に与えられた鍵に、装置の同一性判定機能が含まれていれば、ソフトウェアを不正に複製して他の装置で

40 起動することはできない。
【0053】装置の同一性判定機能が含まれていない場合には、ソフトウェアを不正に複製して他の装置で起動することができるが、期限が来れば使用不能となる。また利用許諾を受けていない者は、更新作業を含む回線経由のサービスは使用できない。また不正使用されたソフトウェアは、ソフトウェアのシリアル番号が登録され、更新・機能の制限を受ける。

【0054】(7) 実際の利用者に対する見え方の例のイメージ

50 図3は本発明の実施例における利用者への見え方（ユー

ザーインタフェース)の例を示す図であって、(a)は販売された直後のソフトウェアの見え方、(b)はその鍵の見え方、(c)は利用者により開錠作業の行われた後のソフトウェアの見え方、(d)は利用者に与えられたソフトウェアの利用免許情報表示の例を示す。

【0055】例えば利用者がオンライン映画情報を購入したとする。図3(a)および(b)に示すように、購入したソフトウェアとその鍵が、購入処理により自分のデスクトップに表示される。ソフトウェアに鍵を入れると、図3(c)に示すように、通常のソフトウェアと同様な起動方法で起動できるようになる。立ち上がり時には、図3(d)に示すように、鍵の持つ利用条件と期限が表示される。この情報は必要なときに見ることができ

る。

【0056】

【発明の効果】以上説明したように、本発明によれば、回線上で購入したソフトウェア等を不正に複製しても、期限が来れば使用不能となり使用できない。またその更新手続きは登録者以外では不可能である。よって、鍵に相当するものを郵送することなく、つまり回線での販売の利便を損うことなく、正規の購入者には最良のメンテナンスサービスを提供しながら、かつ不正利用者の複製利用を時限的に防止することが可能となる。この際の複製利用は、ネットワークプロテクトと異なり、回線から独立していても有効である。

【0057】また、本発明は、試しにある機能だけ使ってみたいとか、ある期間だけ必要であるというような、

従来のソフトウェア販売では対応が困難であった利用者の要求にも柔軟に対応でき、ソフトウェアの市場拡大を促す効果がある。

【0058】また、映画などの著作物についても時限販売、視聴許諾権販売が可能になり、所有を第一目的としない需要、例えば映画を見に行くような需要や、レンタルビデオで借りて見るような需要等にも対応できる。内容を見た結果、再視聴または所有を希望すれば、新たに利用条件を変更、更新することで対処できる。

10 【図面の簡単な説明】

【図1】本発明の実施例のシステム構成図である。

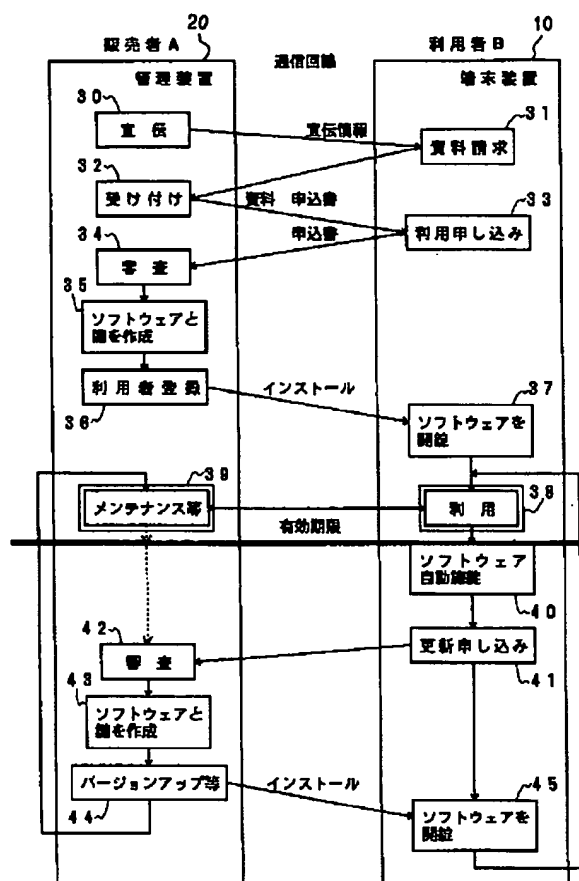
【図2】本発明の実施例による処理の流れを示す図である。

【図3】本発明の実施例における利用者への見え方の例を示す図である。

【符号の説明】

- 10 端末装置
- 11 利用制御手段
- 12 施錠／破壊処理手段
- 13 ソフトウェア／著作物の製品
- 14 継続利用要求処理手段
- 15 開錠／再利用処理手段
- 20 管理装置
- 21 利用者情報管理手段
- 22 資格審査処理手段
- 23 利用権利更新処理手段

【図2】



【図3】

(a)



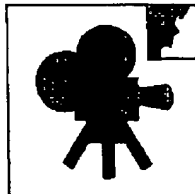
オンライン映画情報

(b)



オンライン映画情報

(c)



オンライン映画情報

(d)

使用免許	××ソフト	許諾ID 25GHAS658JP
初級 試用限定	オンライン映画情報	
	96.7.1から	
	96.8.12 まで	
	佐藤太郎 様 機種○○PC-23	